

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1577802-000

Total Deleted Page(s) = 138

Page 34 ~ Duplicate;
Page 41 ~ b3; b6; b7C; b7E;
Page 42 ~ b3; b6; b7C; b7E;
Page 43 ~ b3; b6; b7C; b7E;
Page 44 ~ b3; b6; b7C; b7D; b7E;
Page 45 ~ b3; b6; b7C; b7E;
Page 46 ~ b3; b6; b7C; b7E;
Page 47 ~ b3; b6; b7C; b7E;
Page 48 ~ b6; b7C; b7E;
Page 49 ~ b3; b6; b7C; b7D; b7E;
Page 50 ~ b5; b6; b7C; b7E;
Page 51 ~ b6; b7C; b7E;
Page 52 ~ b7E;
Page 53 ~ b7E;
Page 54 ~ b7E;
Page 55 ~ b6; b7C; b7E;
Page 115 ~ b3; b7E;
Page 118 ~ b6; b7C; b7E;
Page 119 ~ b6; b7C; b7E;
Page 120 ~ b6; b7C; b7E;
Page 121 ~ b6; b7C; b7E;
Page 122 ~ Duplicate;
Page 123 ~ Duplicate;
Page 124 ~ Duplicate;
Page 125 ~ Duplicate;
Page 126 ~ Duplicate;
Page 128 ~ b6; b7C; b7E;
Page 129 ~ b6; b7C; b7E;
Page 130 ~ b6; b7C; b7E;
Page 131 ~ b6; b7C; b7E;
Page 132 ~ Duplicate;
Page 133 ~ Duplicate;
Page 134 ~ Duplicate;
Page 135 ~ Duplicate;
Page 136 ~ Duplicate;
Page 138 ~ b6; b7C; b7E;
Page 139 ~ b6; b7C; b7E;
Page 140 ~ Duplicate;
Page 141 ~ Duplicate;
Page 142 ~ Duplicate;
Page 144 ~ b6; b7C; b7E;
Page 145 ~ b6; b7C; b7E;
Page 146 ~ Duplicate;
Page 147 ~ Duplicate;
Page 148 ~ Duplicate;
Page 150 ~ b6; b7C; b7E;
Page 151 ~ Duplicate;
Page 152 ~ Duplicate;
Page 154 ~ b6; b7C; b7E;
Page 155 ~ b6; b7C; b7E;
Page 156 ~ Duplicate;
Page 157 ~ Duplicate;
Page 158 ~ Duplicate;
Page 160 ~ b6; b7C; b7E;
Page 161 ~ Duplicate;
Page 162 ~ Duplicate;
Page 164 ~ b6; b7C; b7E;
Page 165 ~ b6; b7C; b7E;
Page 166 ~ Duplicate;
Page 167 ~ Duplicate;
Page 168 ~ Duplicate;
Page 170 ~ b6; b7C; b7E;
Page 171 ~ Duplicate;
Page 172 ~ Duplicate;
Page 174 ~ b6; b7C; b7E;
Page 175 ~ b6; b7C; b7E;
Page 176 ~ b6; b7C; b7E;

Page 177 ~ Duplicate;
Page 178 ~ Duplicate;
Page 179 ~ Duplicate;
Page 180 ~ Duplicate;
Page 182 ~ b6; b7C; b7E;
Page 183 ~ Duplicate;
Page 184 ~ Duplicate;
Page 186 ~ b6; b7C; b7E;
Page 187 ~ Duplicate;
Page 188 ~ Duplicate;
Page 196 ~ b6; b7C; b7E;
Page 197 ~ b6; b7C; b7E;
Page 198 ~ Duplicate;
Page 199 ~ Duplicate;
Page 200 ~ Duplicate;
Page 202 ~ b6; b7C; b7E;
Page 203 ~ b6; b7C; b7E;
Page 204 ~ b7E;
Page 205 ~ b7E;
Page 206 ~ b7E;
Page 207 ~ b7E;
Page 208 ~ b6; b7C; b7E;
Page 209 ~ b6; b7C; b7E;
Page 210 ~ Duplicate;
Page 211 ~ Duplicate;
Page 212 ~ Duplicate;
Page 213 ~ Duplicate;
Page 214 ~ Duplicate;
Page 215 ~ Duplicate;
Page 216 ~ Duplicate;
Page 217 ~ Duplicate;
Page 218 ~ Duplicate;
Page 223 ~ b3; b6; b7C; b7D; b7E;
Page 224 ~ b3; b6; b7C; b7D; b7E;
Page 225 ~ b6; b7C; b7D;
Page 226 ~ b6; b7C; b7D;
Page 227 ~ b6; b7C; b7D;
Page 228 ~ b6; b7C; b7D;
Page 229 ~ Duplicate;
Page 230 ~ Duplicate;
Page 232 ~ b3; b6; b7C; b7D; b7E;
Page 233 ~ b6; b7C; b7D;
Page 234 ~ b6; b7C; b7D;
Page 235 ~ b6; b7C; b7D;
Page 236 ~ b6; b7C; b7D;
Page 237 ~ b6; b7C; b7D;
Page 238 ~ b6; b7C; b7D;
Page 239 ~ b6; b7C; b7D;
Page 240 ~ b6; b7C; b7D;
Page 242 ~ Duplicate;
Page 243 ~ Duplicate;
Page 244 ~ Duplicate;
Page 245 ~ Duplicate;
Page 246 ~ Duplicate;
Page 247 ~ Duplicate;
Page 248 ~ Duplicate;
Page 249 ~ Duplicate;
Page 250 ~ Duplicate;
Page 252 ~ b6; b7C; b7D;
Page 253 ~ b6; b7C; b7D;
Page 254 ~ b6; b7C; b7D;
Page 256 ~ b6; b7C; b7D;
Page 257 ~ b6; b7C; b7D;
Page 258 ~ b6; b7C; b7D;
Page 259 ~ b6; b7C; b7D;
Page 260 ~ b6; b7C; b7D;
Page 261 ~ b7D;
Page 262 ~ Duplicate;
Page 270 ~ b6; b7C; b7E;
Page 271 ~ Duplicate;
Page 272 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

File - Serial Charge Out
FD-5 (Rev. 10-13-89)

Date _____

b3

b7E

File _____

Class. _____

Office of Origin _____

Case No. _____

Last Serial _____

☐ Pending

☐ Closed

Serial No. _____

Description of Serial _____

Date
Charged _____

417

Employee _____

RECHARGE

Date _____

To _____ From _____

Initials of
Clerk

{ _____

_____ }

Date

{ _____

_____ }

Date charged _____

Employee _____

Location _____

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/05/2000

To: Seattle✓

From: Seattle

Squad 11

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (None)

Title: UNSUB, a.k.a.

[redacted]
LIGHTREALM, INC
SEATTLE, WASHINGTON - VICTIM;
CITA - INTRUSION

Synopsis: Open case on titled matter.

Details: On 12/13/99, [redacted] was arrested in Reno, NV for receiving goods from Amazon.com and other Internet retailers that were purchased with stolen credit card numbers [redacted]

[redacted] The orders were placed from computers in Russia. Investigation has determined it is probable that the card numbers were obtained from hacked computers at Lightrealm, Inc., an ISP located in Seattle, WA. Investigations by other Divisions have determined that a [redacted] has gained access to Lightrealm's system and may have stolen credit card numbers from their database.

It is recommended that a case be opened on titled matter and assigned to SA [redacted]

157 [redacted] 01.ec

b3
b6
b7C
b7E

17
[redacted]

b3
b6
b7C
b7E

b6
b7C
b7E

[redacted]

SA
11/100
[redacted]

[redacted]

6/5/00

11/01/01
19:32:16

FD-192

ICMIPR01
Page 1

Title and Character of Case:

FLYHOOK
[REDACTED]

Date Property Acquired: 11/10/2000
Source from which Property Acquired:
FROM SEIZED TOSHIBA LAPTOP & UC THINKPAD & UC DELL

Anticipated Disposition: Acquired By: [REDACTED]

Case Agent: [REDACTED]

Description of Property:
1B 15

Date Entered

TWO (2) ORIGINAL LAPTOP HARD DRIVES:

2. IBM TRAVELSTAR MODEL DARA-206000 6.00 GB FROM DELL LAPTOP
(FBI UC) INSPIRON 7500 PN 0009963T-12961-04F-1485

b6
b7C
b7E

3. IBM TRAVELSTAR MODEL DBCA-206480 6.44 GB FROM IBM
THINKPAD (FBI UC) [REDACTED]

Barcode: E01688317 Location: ECC1 272 01/23/2001

ONE (1) ORIGINAL LAPTOP HARD DRIVE:

1) IBM TRAVELSTAR MODEL DBCA-206480 6.49 GB SN/RRPJ5518 FROM
TOSHIBA LAPTOP (SUBJECT MACHINE) #X9162243A

Barcode: E01847382 Location: ECC1 272 11/01/2001

① [REDACTED]

② FILE

Case Number: [REDACTED]
Owning Office: SEATTLE [REDACTED]

b3
b6
b7C
b7E

SEARCHED [REDACTED] INDEXED [REDACTED]
SERIALIZED [REDACTED] FILED [REDACTED]
NOV 01 2001
FBI SEA [REDACTED]

File

08/01/00
12:31:24

FD-192

ICMIPR01
Page 1

Title and Character of Case:

LIGHTREALM INC

Date Property Acquired: 07/14/2000
Source from which Property Acquired:
ORIGINAL ELSUR RECORDING

Anticipated Disposition: Acquired By: Case Agent:

b6
b7c

Description of Property:
1D 1

Date Entered

TAPE #1, 7/14/00, TCM W/

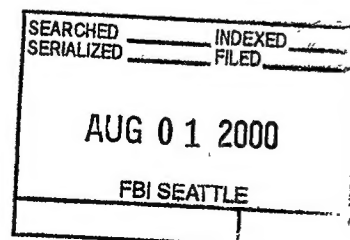
Barcode: E1770204

Location: ELSUR I

08/01/2000

Case Number:
Owning Office: SEATTLE

b3
b7E



FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 06/12/2000

To: Counterterrorism

Attn:

Investigative Services
Los Angeles
Moscow
Newark

Seattle

SSA [redacted]
IOS [redacted]
SARA-3, SA [redacted]
ALAT [redacted]
Franklin Township RA
SA [redacted]
SA [redacted]
SA [redacted]

b6
b7C
b7E

From: New Haven

6

Contact: [redacted]

Approved By [redacted]

Drafted By [redacted]

Case ID #: [redacted]

b3
b6
b7C
b7E

Title: UNSUB, aka [redacted] Fug (B);
OIB, Inc. - Victim;
Impairment, Intrusion, Extortion

Synopsis: Confirmation of DCM, Moscow Embassy permission for lure proposal of captioned subject.

Reference: [redacted]

b3
b6
b7C
b7E

Details: Captioned subject, [redacted] has been identified as having gained unauthorized access to multiple computers and to have attempted to extort computer related businesses, to include OIB, Vernon, Connecticut. New Haven Division has obtained an arrest warrant for [redacted] is currently believed to be in Chelyabinsk, Russia.

Referenced New Haven electronic communication (ec) set out details for a proposed lure to lure [redacted] to the United States. This lure was discussed by secure telephone conversation with ALAT [redacted] Moscow on 6/16/2000.

JUN 21 2000

FBI SEATTLE [redacted]

To: Counterterrorism From: New Haven
Re: [REDACTED] 06/12/2000

b3
b6
b7C
b7E

On 6/20/2000, ALAT [REDACTED] advised that the Deputy
Chief of Mission, Moscow Embassy, had posed no objection to the
FBI lure proposal.

To: Counterterrorism From: New Haven
Re: [REDACTED] 06/12/2000

b3
b7E

LEAD(s) :

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

[REDACTED] is requested to review and authorize this
[REDACTED]

Set Lead 2:

LOS ANGELES

AT Santa Anna, California

Read and clear.

Set Lead 3:

NEWARK

AT FRANKLIN TOWNSHIP, NEW JERSEY

Read and clear.

Set Lead 4:

SEATTLE

AT SEATTLE, WASHINGTON

Read and clear.

Set Lead 5:

MOSCOW

AT MOSCOW, RUSSIA

Read and clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 07/19/2000

To: Criminal Investigative

Attn: Undercover and Sensitive
Operations Unit (USOU),

SSA [REDACTED]
SSA [REDACTED]

Seattle

From: Seattle

Squad 11

Contact: SA [REDACTED]

Approved [REDACTED]

Drafted [REDACTED]

Case ID [REDACTED]

Title: UNSUB, aka

[REDACTED]
LIGHTREALM, INC
SEATTLE, WASHINGTON - VICTIM;
CITA - INTRUSION

b3
b6
b7C
b7E

Synopsis: Request Undercover and Sensitive Operations Unit (USOU) review their database to find an Undercover Agent (UCA) for a Group II Undercover Operation (UCO) in the Seattle Division.

Details: The Seattle Division is awaiting approval of a Group II UCO, the objective being [REDACTED]

[REDACTED] is a Russian hacker who has been charged by Complaint in the District of Connecticut with illegally intruding into a computer [REDACTED]. [REDACTED] is also believed to have hacked into computers and extorted or attempted to extort money from companies located in the Newark [REDACTED] Los Angeles [REDACTED] and Seattle [REDACTED] Divisions.

b3
b6
b7C
b7E

Seattle's Group II UCO scenario is as follows: [REDACTED]

b3
b6
b7C
b7D
b7E

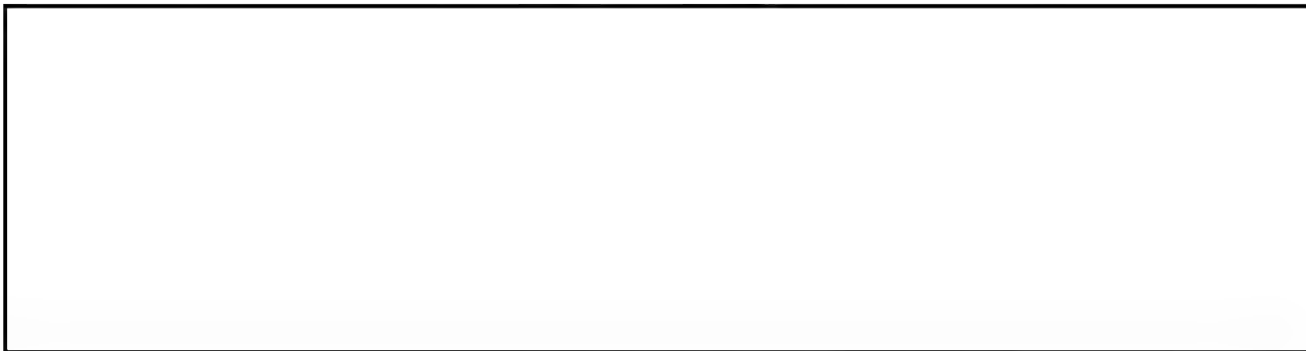
SEARCHED
SERIALIZED

INDEXED
FILED

JUL 20 2000

SEAT

To: Criminal Investigative From: Seattle
Re: [REDACTED] 07/19/2000



b3
b6
b7C
b7E

To: Criminal Investigative From: Seattle
Re: [REDACTED] 07/19/2000

b3
b7E

LEAD(s):

Set Lead 1:

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

Advise Seattle of the availability of a UCA with computer capabilities and an understanding of the Russian language.

20 [REDACTED] 01.ec
♦♦

b6
b7C

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/31/2000

To: Seattle

From: Seattle

Squad 11

Contact: SA [REDACTED]

Approved By [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

Title: CHANGED
FLYHOOK;
CIDT - INTRUSION

Synopsis: Change title to reflect code name FLYHOOK.

Previous Title: Title marked "Changed" to reflect code name FLYHOOK. Title previously carried as "UNSUB(S), a.k.a. [REDACTED] LIGHTREALM, INC., SEATTLE, WASHINGTON - VICTIM; CIDT - INTRUSION."

Details: The purpose of this EC is to change the title of this case. On 7/27/00, a Group II proposal was approved changing the title to the code name FLYHOOK.

213 [REDACTED] 01.ec

♦♦

b3
b6
b7C
b7E

(Handwritten mark)

b6
b7C

[REDACTED]

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/01/2000

To: New Haven
Newark
Seattle

Attn: SA [redacted]
SA
SA

From: Los Angeles
SARA 3

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]
[redacted]

Title: UNSUB(S) aka [redacted] Fug (B);
OIB, Inc. - Victim;
Impairment, Intrusion, Extortion

Synopsis: Lead covered in Los Angeles.

Reference: [redacted]
9A-NK-102430 Serial 17
[redacted]

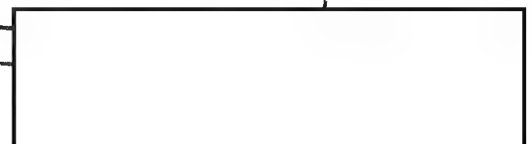
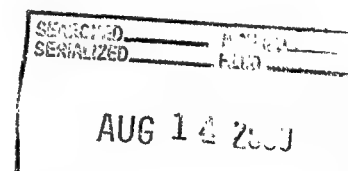
Details: The [redacted] has been reviewed and all changes have been communicated telephonically to SA [redacted] in New Haven Division on 06/20/2000.

♦♦

b3
b6
b7C
b7E

(X)

b3
b6
b7C
b7E



FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/01/2000

To: Criminal Investigative
Counterterrorism

Attn: Unit Chief [redacted]
SSA [redacted]
SSA [redacted]
UCC [redacted]
SSA [redacted]

b3
b6
b7C
b7E

Salt Lake City

From: Seattle

Squad 5

Contact: SSA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: FLYHOOK;
COMPUTER INTRUSION

Synopsis: To confirm with CID and Salt Lake City the usage of SA [redacted] as a UCA on the captioned Group II UCO.

Details: For the information of CID, Counterterrorism, and Salt Lake City, the captioned Group II UCO [redacted]

[redacted]
States for arrest and prosecution on the charges of computer intrusion in the United States. An arrest warrant has been issued for [redacted] from the District of Connecticut charging him with fraud and related activity in connection with computers in violation of Title 18, USC, Section 1030. This case is one of a series of [redacted] involving Russian hackers being handled by the Seattle, New Haven, Los Angeles, Sacramento, Newark, and Washington Field Office divisions.

b3
b6
b7C
b7E

Seattle envisions SA [redacted]

[redacted]

To: Criminal Investigative From: Seattle
Re: [redacted] 08/01/2000

b3
b6
b7C
b7E

Seattle envisions using SA [redacted] for a one week period during late August 2000 or early September 2000.

All travel costs will be paid by Seattle Group II UCO funds. SA [redacted] should travel to Seattle in an undercover capacity.

To: Criminal Investigative From: Seattle
Re: [REDACTED] 08/01/2000

b3
b7E

LEAD(s):

Set Lead 1:

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

For your information.

Set Lead 2:

COUNTERTERRORISM

AT WASHINGTON, DC

For your information.

Set Lead 3:

SALT LAKE CITY

AT SALT LAKE CITY, UTAH

For your information.

214 [REDACTED] 01.ec

◆◆

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/02/2000

To: Criminal Investigative
Counterterrorism

Attn: SSA [redacted]
SSA [redacted]
SSA [redacted]

USOU [redacted]

From: Seattle

Squad 5 [redacted]

Contact: SSA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID # [redacted]

Title: FLYHOOK;
COMPUTER INTRUSION

b3
b6
b7C
b7E

Synopsis: To report the findings of the Seattle Division's Criminal Undercover Operation Review Committee (CUORC).

Enclosure(s): Enclosed for CID and Counterterrorism are two approved copies of the captioned Group II proposal.

Details: On 07/27/2000, the proposed Group II Undercover Operation (UCO), "FLYHOOK", was presented to the Division CUORC for approval by Special Agent [redacted]. The following CUORC members were present:

b6
b7C
b7E

ASAC [redacted]
UCC [redacted]
SSA [redacted]
SSA [redacted]
SSA [redacted]

(Squad Supervisor of the proposed UCO)

Informant Coordinator [redacted]
CDC [redacted]
FM [redacted]

Additionally, Co-Case Agents [redacted] and [redacted] were present at the meeting.



To: Criminal Investigative From: Seattle
Re: [REDACTED] 08/02/2000

Approval/Action

b3
b7E

The Committee recommended that FLYHOOK be approved by SAC, Seattle, as a Group II UCO on 08/01/2000. SAC, Seattle, approved FLYHOOK as a Group II UCO with an operation budget of [REDACTED]. No extraordinary risk of injury, loss of property, or civil liability is anticipated during the operation of this UCO.

Seattle Division management and case personnel should be aware of the following general stipulations:

(1) All FBI agents used as UCA's must be Bureau Certified UCA's. All Bureau UCA's must receive Undercover Safeguard Unit assessment every six months while involved in an undercover capacity.

(2) All investigations conducted outside of the United States and in foreign territory must be in accordance with the Attorney General Guidelines or Extraterritorial Activities.

To: Criminal Investigative From: Seattle
Re: [REDACTED] 08/02/2000

b3
b6
b7C
b7E

LEAD(s) :

Set Lead 1:

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

For your information.

Set Lead 2:

COUNTERTERRORISM

AT WASHINGTON, DC

For your information.

219 [REDACTED] 01.ec
♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/31/2000

To: Counter terrorism

Attn:

	SSA	
	SSA	
	SSA	
	IOS	

Investigative Services
Legat Moscow
Los Angeles

Newark
New Haven

Sacramento
✓ Seattle

TOUL-1

SA
SA
SA
SA
SA
SA
SA
SA

b6
b7C
b7E

From: Little Rock
Squad 3

Contact: SA

501-228-8529

Approved By:

Drafted By:

Case ID #:



Title: UNSUB(S);

FBW

b3
b6
b7C
b7E

Synopsis: To update offices of recent information.

Enclosures: Enclosed for receiving offices are [redacted]
received from [redacted] in San Diego, California. These
[redacted] are further identified in the details section of this
EC.

b3

SEARCHED
SERIALIZED

AUG 15 2000

To: Counter terrorism From: Little Rock
Re: [REDACTED] 07/31/2000

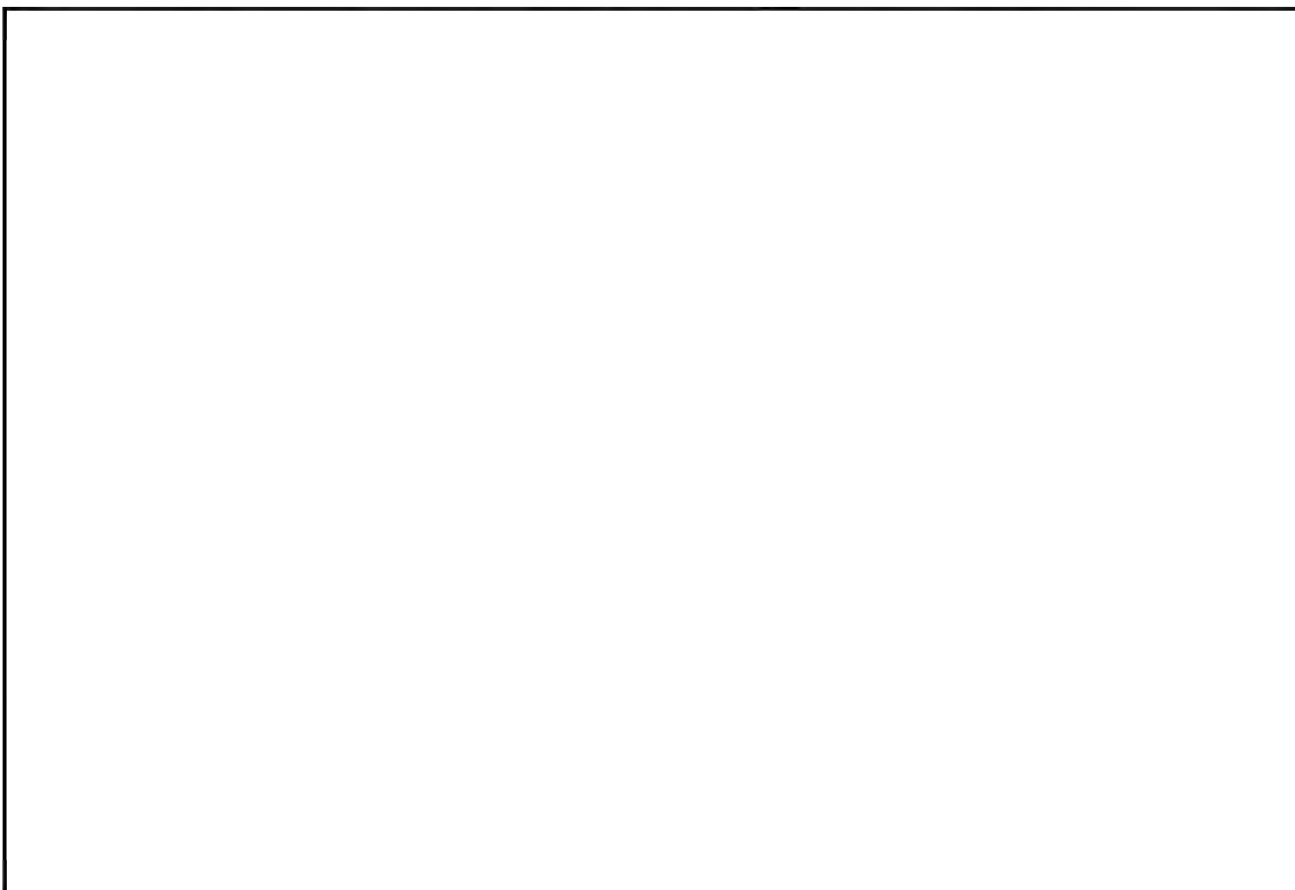
b7E

Details: A lead was recently covered in the San Diego, California area. The details of this lead are as follows. A couple of names and addresses were revealed from lead which hopefully can be of assistance.

A brief background regarding this latest lead. In December of 1999, an auction website at America On Line (AOL) was used by UNSUB(S) in above captioned case. The purpose of this auction site was allegedly to offer computer equipment for sale through a company calling itself [REDACTED]. The individual(s) setting up this auction site presented to AOL a credit card in which to pay for the site. The credit card came back to a [REDACTED] of Longview, Washington. [REDACTED] advised he had several unauthorized transactions on his credit card around this time.

b6
b7C

The few persons who actually bid on this equipment were informed via e-mail to wire transfer money through an account in New York and ultimately into Hansabanka, Riga, Latvia, the account of International Metal Trading Bank.



b3
b6
b7C

To: Counter terrorism From: Little Rock
Re: [REDACTED] 07/31/2000



♦♦

b3
b6
b7C
b7E

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 08/24/00 Time: 16:30

Case ID:

Description of Document:

Type : OUTLET

Date : 08/02/00

To : NETWRK COMP

From : SEATTLE

Topic: PRESERVATION OF EVIDENCE

Reason for Permanent Charge-Out:

wrong file number on document

Transferred to:

Case ID:

Employee:

b3
b6
b7C
b7E

08/24/2000
16:08:53

Permanent Charge-Out of Serial

ICMLPE20
Page 1

***** Permanent Charge-Out of Serials Summary *****

There are no leads for old Case ID with Serial 14 to be copied

b3
b7E

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/21/2000

To: Counterterrorism

Attn:

SSA
SSA
IOS

Little Rock
Los Angeles

New Haven

Sacramento
Seattle

Washington Field

SA
SA
SA
SA
SA
SA
SA
SA

From: Newark

Franklin Township Resident Agency/Squad 2

Contact: SA [redacted] 732/805-0463, ext. 271

Approved By:

Drafted By:

Case ID #:

b3
b6
b7C
b7E

Title: UNSUB(s). aka.

[redacted]
ET AL.;
FINANCIAL SERVICES, INC.,
GLEN ROCK, NEW JERSEY - VICTIM;
INTRUSION - INFORMATION SYSTEMS
THEFT OF INFORMATION - INFORMATION SYSTEMS
EXTORTION - INFORMATION SYSTEMS

SEARCHED _____	INDEXED _____
SERIALIZED _____	FILED _____
AUG 30 2000	
FBI - SEATTLE	

To: Counterterrorism From: Newark
Re: [REDACTED] 08/21/2000

Enclosure(s): For each substantive case file, one set of electronic mail and ICQ messages from [REDACTED] to [REDACTED]. Multiple messages are provided in date order from 07/25/2000 through 03/29/2000.

Synopsis: To provide for comparison purposes, electronic mail and ICQ messages exchanged between [REDACTED] (LNU), aka [REDACTED] and FBI Newark victim company.

Details: By way of background, all captioned investigations relate to the computer intrusion and extortion of victim companies by an individual(s) named [REDACTED]

FBI Newark's victim, Financial Services, Inc. exchanged several communications with the subject, beginning in March 2000 and ending in July 2000. These are documented to the Newark substantive case file, but not available for review in ACS because they are enclosed in 1A envelopes.

To assist in further identifying [REDACTED] and linking the referenced substantive case files, these communications are being made available to the captioned Case Agents for use as appropriate in the respective investigations.

◆◆

b3
b6
b7C
b7E

Received: from mail.sitek.net [212.34.32.37] mail.fsiwebs.com with ESMTP

(SMTPD32-6.00) id A9883060114; Mon, 24 Jul 2000 17:47:52 -0400

Received: from mail.sitek.net (t2-10.sitek.net [212.34.33.73])

by mail.sitek.net (8.9.2/8.9.1) with SMTP id BAA02273

for [REDACTED]; Tue, 25 Jul 2000 01:52:19 +0400

(MSD)

Date: Tue, 25 Jul 2000 01:53:04 -0700

From: [REDACTED]

X-Mailer: The Bat! (v1.029) S/N 83DA2C20

Reply-To: [REDACTED]

Priority: Normal

Message-ID: <1378.000725@doctor.com>

To: [REDACTED]

Subject: Re[2]: Hello this is [REDACTED] your security "agent" that was patched your system some months ago

References: <0FD0E3F4F664D211B2BF0000F6B9864BF2242D@EXCHANGE>

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: <[REDACTED]>

X-UIDL: 260988921

Status: U

b6
b7c

Received: from 206.142.23.12 [206.142.23.12] by in3.prserv.net id 965055389.83398-1 ; Mon, 31 Jul 2000 14:56:30 +0000

Received: from EXCHANGE by [206.142.23.12]

via smtpd (for in3.prserv.net [32.97.166.46]) with SMTP; 1 Apr 2000 15:45:14 UT

Received: by EXCHANGE with Internet Mail Service (5.5.2650.21)

id <PZ90W1BN>; Mon, 31 Jul 2000 10:53:24 -0400

Message-ID: <0FD0E3F4F664D211B2BF0000F6B9864BBAEA30@EXCHANGE>

From: [REDACTED]

To: "

Subject: FW: FRG - [REDACTED]

Date: Mon, 31 Jul 2000 10:53:23 -0400

Return-Receipt-To: [REDACTED]

MIME-Version: 1.0

X-Mailer: Internet Mail Service (5.5.2650.21)

Content-Type: text/plain

FYI

> -----Original Message-----

> From: [REDACTED]

> Sent: Monday, July 31, 2000 9:29 AM

> To: [REDACTED]

> Subject: FRG - [REDACTED]

>

>

> -----Original Message-----

> From: [REDACTED]

> Sent: Tuesday, July 25, 2000 4:53 AM

> To: [REDACTED]

> Subject: Re[2]: Hello this is [REDACTED] your security "agent" that was

> patched your system some months ago

>

> Hello [REDACTED]

>

> [REDACTED] Hi [REDACTED]

> [REDACTED] With your help, I thought we plugged all the holes. What did you

> find?

> Yes, ofcource, byt date by date, time by time hackers founding new holes

> in NT, that's why i am writing u.

> i will email u back tomorrow with writing about your hole.

> cya

>

> Best regards,

[REDACTED]

mailto:[REDACTED]

b6
b7c

b6
b7c

Received: from mail.sitek.net [212.34.32.37] by [REDACTED] w
ith ESMTP

(SMTPD32-6.00) id A521A0146; Sat, 22 Jul 2000 06:19:13 -0400

Received: from mail.sitek.net (t2-30.sitek.net [212.34.33.93])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id OAA16552
for [REDACTED]; Sat, 22 Jul 2000 14:23:48 +0400

(MSD)

Date: Sat, 22 Jul 2000 14:20:21 -0700

From: [REDACTED]

X-Mailer: The Bat! (v1.029) S/N 83DA2C20

Reply-To: [REDACTED]

Priority: Normal

Message-ID: [REDACTED]

To: [REDACTED]

Subject: Hello this is [REDACTED] your security "agent" that was patche
d your system some months ago

References: <000e01bfaec6\$9f9b3590\$05f188cd@frankgvp>

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: [REDACTED]

X-UIDL: 260988901

Status: U

b6
b7c

31 Jul 2000 14:55:55 +0000

Received: from EXCHANGE by [206.142.23.12]

via smtpd (for in2.pr.v.net [32.97.166.45]) with SMTP; 1 Jul 2000 15:44:39 UT

Received: by EXCHANGE with Internet Mail Service (5.5.2650.21)

id <PZ90W1BK>; Mon, 31 Jul 2000 10:52:49 -0400

Message-ID: <0FD0E3F4F664D211B2BF0000F6B9864BBAEA2F@EXCHANGE>

From: [REDACTED]

To: "

Subject: FW: FRG to ALEX I

Date: Mon, 31 Jul 2000 10:52:48 -0400

Return-Receipt-To: [REDACTED]

MIME-Version: 1.0

X-Mailer: Internet Mail Service (5.5.2650.21)

Content-Type: text/plain

FYI

> -----Original Message-----

> From: [REDACTED]

> Sent: Monday, July 31, 2000 9:29 AM

> To: [REDACTED]

> Subject: FRG to [REDACTED]

> -----Original Message-----

> From: [REDACTED]

> Sent: Monday, July 24, 2000 3:03 PM

> To: [REDACTED]

> Subject: RE: Hello this is [REDACTED] your security "agent" that was

> patched your system some months ago

>

> Hi [REDACTED]

> With your help, I thought we plugged all the holes. What did you find?

> Thanks,

> [REDACTED]

> -----Original Message-----

> From: [REDACTED]

> Sent: Saturday, July 22, 2000 5:20 PM

> To: [REDACTED]

> Subject: Hello this is [REDACTED] your security "agent" that was patched

> your system some months ago

>

> Hello [REDACTED]

>

> [REDACTED] i would like to talk with u over the net.

> I was found one new hole in your system and want to contact u asap.

> cya

>

> Best regards,

> [REDACTED]

>

>

b6

b7c

b6

b7c

FROM [REDACTED]

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTP
(SMTPD32-6.00) id AE787AEF003E; Fri, 05 May 2000 10:45:12 -0400
Received: from mail.sitek.net (t1-51.sitek.net [212.34.32.114])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id SAA18996
for [REDACTED]; Fri, 5 May 2000 18:43:21 +0400 (MSD)

Date: Fri, 5 May 2000 18:42:47 -0700

From: [REDACTED]

X-Mailer: The Bat! (v1.029) S/N 83DA2C20

Reply-To: [REDACTED]

Organization: Internet Security

Priority: Normal

Message-ID: <16779.000505@doctor.com>

To: [REDACTED]

Subject: Re[2]: FSI

References: <000901bfb5cc\$2f72c5f0\$05f188cd@ [REDACTED]>

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: [REDACTED]

X-UIDL: 254610894

Status: U

Hello [REDACTED]

Hi, hello what is the steps of our next work ?

Best regards,

mailto:[REDACTED]

E
S
I
T
E
B
E
E
W
R
J
O
Y
E
R
E
H
W

Untitled

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTP
(SMTPD32-6.00) id A77D18A024C; Thu, 04 May 2000 20:36:13 -0400
Received: from mail.sitek.net (megz@t2-24.sitek.net [212.34.33.87])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id EAA19246
for [REDACTED]; Fri, 5 May 2000 04:34:22 +0400 (MSD)

Date: Fri, 5 May 2000 04:33:49 -0700

From: [REDACTED]

X-Mailer: The Bat! (V1.029) S/N 83DA2C20

Reply-To: [REDACTED]

Organization: Internet Security

Priority: Normal

Message-ID: [REDACTED]

To: [REDACTED]

Subject: Re[2]: FSI

References: <000901bfb5cc\$2f72c5f0\$05f188cd@ [REDACTED]>

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: [REDACTED]

X-UIDL: 254610884

Status: U

Hello [REDACTED]

b6
b7c

Ok, money have come



mailto:[REDACTED]

E
I
S
B
E
W

R
J
O
Y

E
R
E
H
W

Untitled

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTP
(SMTPD32-6.00) id ACB757501EA; Thu, 04 May 2000 13:00:39 -0400
Received: from mail.sitek.net (t1-35.sitek.net [212.34.32.98])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id UAA01777
for [redacted] Thu, 4 May 2000 20:58:49 +0400 (MSD)

Date: Thu, 4 May 2000 20:58:17 -0700

From: [redacted]

X-Mailer: The Bat! (v1.020) S/N 835A7C20

Reply-To: [redacted]

Organization: Internet Security

Priority: Normal

Message-ID: [redacted]

To: 'mgeluso' [redacted]

Subject: Re[2]: FSI

References: <000901bfb5cc\$2f72c5f0\$05f188cd@ [redacted]>

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: [redacted]

X-UIDL: 254610872

Status: U

Hello [redacted]

b6
b7c

f> Maybe the CHIPS type tranfer will take longer? Like the 3 to 5 days us told
f> us about before? The money was sent 10:00 am Tuesday May 02 our time, using
f> the same information. The only difference is it was sent CHIPS, instead of

FsiWebs

Really i first time here term of CHIPS .

But i will wait for money.

W

T

Best regards

mailto:[redacted]

W

W

>

R

J

O

>

W

R

W

T

W

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTTP (SMTPD32-6.00) id ABFD188C0068; Thu, 04 May 2000 03:51:25 -0400
Received: from mail.sitek.net (t1-10.sitek.net [212.34.32.73])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id LAA19649
for [REDACTED]; Thu, 4 May 2000 11:49:22 +0400 (MSD)

He110

Hello

have checked account
still no money on account
can u check it ?

mailto:

W
I
W
R
W
Y
O
J
R
W
E
E
E

Untitled

From: [REDACTED]

To: [REDACTED]

Subject: PSI

Date: Tue, 2 May 2000 10:55:49 -0400

MIME-Version: 1.0

Content-Type: text/plain;
charset="iso-8859-1"

Content-Transfer-Encoding: 7bit

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 5.00.2919.6700

X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6700

H: [REDACTED]

Wire transfer sent this morning 10:00 am transfer seq. # 2055.

b6
b7C

Note: Bank would not use SWIFT code (IRVTUS3N).

Used CHIP # 0001, bank indicated that this is the SWIFT code equivalent.

Let me know when you receive the \$2K.

[REDACTED]

Untitled

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMT
(SMTPD32-6.00) id AC11630C0138; Fri, 28 Apr 2000 02:13:37 -0400
Received: from mail.sitek.net (megz@t2-14.sitek.net [212.34.33.77])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id KAA04557
for [redacted] Fri, 28 Apr 2000 10:13:32 +0400 (MSD)

Date: Fri, 28 Apr 2000 10:11:21 -0700
From: [redacted]
X-Mailer: The Bat! (v1.029) S/N 83DA2C20
Reply-To: [redacted]
Organization: Internet Security
Priority: Normal
Message-ID: [redacted]
To: [redacted]
Subject: Scan of your network
References: <003c01bfafb5\$797a9000\$05f188cd@ [redacted]>
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-RCPT-TO: [redacted]
X-UIDL: 254610792
Status: U

Hello [redacted]

Hello, i was made today SYN stealth scan of your network and i see
that everything ok, and i was not able to enter to your system.

U don't have any holes in your system.

And i am waiting for the end of my part and what to talk with u about
future business.

cya

f> Regarding the below question, we want to know what you 'deposited' on our
f> system, not removed.

f> "2. what files did you leave on our systems(s). We want to make sure we
f> have found and removed all of them."

f> We need to make sure that all of these elements are removed before your
f> test.

f> [redacted]

Best regards,

mailto:[redacted]

b6
b7C

Untitled

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMT
(SMTPD32-6.00) id A3667F3F0142; Thu, 27 Apr 2000 08:32:38 -0400
Received: from mail.sitek.net (megz@t2-58.sitek.net [212.34.33.121])
by mail sitek net (8.9.2/8.9.1) with SMTP id QAA10556
for [REDACTED] Thu, 27 Apr 2000 16:32:24 +0400 (MSD)

Date: Thu, 27 Apr 2000 16:30:19 -0700
From: [REDACTED]
X-Mailer: The Bat! (v1.029) S/N 83DA2C20
Reply-To: [REDACTED]
Organization: Internet Security
Priority: Normal
Message-ID: [REDACTED]
To: [REDACTED]
Subject: Re: PSI
References: <003c01bfafb5\$797a9000\$05f188cd@ [REDACTED]>
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-RCPT-TO: [REDACTED]
X-UIDL: 254610782
Status: U

Hello [REDACTED]

Ah..

Ok.

I didn't understand first time question, sorry.

My files is :

- 1) winnt\system32\system2 - this full dir with all files in it
(not on all computerz exist)
- 2) winnt\system32\pslist.exe
kill.exe
ntalert.exe
pwdump.exe
smmsniff.exe
mount.exe
w32n50.dll
pcandis3.vxd
pcandis4.sys
pcandis5.sys

f> Regarding the below question, we want to know what you 'deposited' on our
f> system, not removed.

f> "2. What files did you leave on our systems(s). We want to make sure we
f> have found and removed all of them."

From: [REDACTED]
To: [REDACTED] 0426_HEADERS
Subject: FSI
Date: Wed, 26 Apr 2000 15:27:34 -0400
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6700
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6700

Hi [REDACTED]

Regarding the below question, we want to know what you 'deposited' on our system, not removed.

"2. What files did you leave on our systems(s). We want to make sure we have found and removed all of them."

We need to make sure that all of these elements are removed before your test.

[REDACTED]

b6
b7C

Untitled
Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTP
(SMTPD32-6.00) id AEDB33402A4; Tue, 25 Apr 2000 15:15:39 -0400
Received: from mail.sitek.net (t2-32.sitek.net [212.34.33.95])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id XAA23657
for [REDACTED] Tue, 25 Apr 2000 23:15:34 +0400 (MSD)
Date: Tue, 25 Apr 2000 23:15:30 -0700
From: [REDACTED]
X-Mailer: The Bat! (v1.029) 5/N 83DA2C20
Reply-To: [REDACTED]
Organization: Internet Security
Priority: Normal
Message-ID: <5967.000425@doctor.com>
To: "fgeluso" [REDACTED]
Subject: Re[2]: WHERE ARE U ?????
References: <000e01bfaec6\$9f9b3590\$05f188cdd [REDACTED]>
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-RCPT-TO: [REDACTED]
X-UIDL: 254610752
Status: U

b6
b7C

Hello [REDACTED]

f> Hi [REDACTED]

f> Sorry I did not get back to you yesterday when I returned to work, but we
f> are still working and I wanted to find out where we stood.

f> [REDACTED] it was real cool what you achieved with us. I would like to know the
f> following:

f> 1. what exactly were the method(s) you used to enter our system. I would
f> like to know how you got in and what you did to get our passwords and
f> navigate
f> throughout our network and also how you transferred data to your
f> location.

Ok it's easy.

- 1) Scanning for wellknown in hacker world "holes" (it was IIS in some computerz)
(also u was have other holes, but it was the easiest.
- 2) after installing of backdoor to your system i was copied all your passwords. And huh ;)
- 3) Decoding passwords (need 3 hourz on my DuAL IP3-700 ;) and making password list.
- 4) After making 3 steps i was impressed that password are the same on ~ all computerz in your network. and u was have NETBIOS over TCP/IP ..
So i was able to start service on your NT computer
and also upload/dl info. and a lot of admin users instead of Administrator on NT computer, it was for me surprise ... After i was entered to your ns1 server [REDACTED] - and have seen that u have intranet ..
;) i was wrote in 2 horz scanner and uploaded it to ns1. after it i was all your computeerz in your network (also i have map in my house of your computer network, wroten on the paper ;).
- 5) hmm u think how was i able to download info from intranet ? ;) it don't have route to internet, huh ... really how ? and how i was able to run backdoor in intranet ? ;) i was wrote NT-Gate programm, that was roam all info from port_1 to port2_of_ip_2 ... and also was made my local computer as Backup Domain Controller ;)
- 6) To know passwords that i was not able to know - i was used Sniffer programs

Untitled

for Token Ring network.

f> 2. What files did you leave on our systems(s). We want to make sure we
f> have found and removed all of them.

I have huge of other interested info from other compoanyes and i don't
need your files. (i don't save garbage in my hdd ;) So i will delete
all that consist your info after the end of the deal .

f> 3. Can you also submit a full list of the materials you have. I know you
f> said it was alot but I need this information.

It's very verrrryyy difficult.

I can say u that i was have access to all your computerz, and what was
i see interested for me - i was packed it and copy to my arhive... the
arhive is very Huge and large.

I forgot to say u - i also was have AMEX soft...from your computer,
but it was need password, so , my friend was cracked it - but i don't
need any fraud and other doing. I am working on security and nothing
more.

f> Also:

f> We are also willing to participate in your testing of our security but
f> would like to schedule it at a set time frame and date.
You want to see what methods i will use ? where from will i scan your
network and otherz ? ;)
Ok, i really don't know when , i don't have any timetable for hacker
attacks.

f> How much time will you need and when?

I need not more then 15 mins, couse u have only 2 computerz that have
route to your Intranet, other computerz not interesting ;)

Cya, and wanna work with u, also waiting for 2k\$.

cya

Best regards

[Redacted]

mailto:

[Redacted]

b6
b7C

From: [REDACTED] Untitled
To: [REDACTED]
References: <001501bfa3c9\$60938da0\$09f188cd@fsiwebs.net> [REDACTED]
Subject: Re: WHERE ARE U ?????
Date: Tue, 25 Apr 2000 10:57:49 -0400
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6700
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6700

Hi [REDACTED]

Sorry I did not get back to you yesterday when I returned to work, but we are still working and I wanted to find out where we stood.

[REDACTED] it was real cool what you achieved with us. I would like to know the following:

b6
b7C

1. What exactly were the method(s) you used to enter our system. I would like to know how you got in and what you did to get our passwords and navigate throughout our network and also how you transferred data to your location.

2. What files did you leave on our systems(s). We want to make sure we have found and removed all of them.

3. Can you also submit a full list of the materials you have. I know you said it was alot but I need this information.

Also:

We are also willing to participate in your testing of our security but would like to schedule it at a set time frame and date.
How much time will you need and when?

[REDACTED]

FROM [REDACTED] HEADERS
Received: from mail.sitek.net [212.34.32.37] by mail.fsiwts.com with ESMT
(SMTPD32-6.00) id AE623601AA; Sun, 23 Apr 2000 15:26:21 -0400
Received: from mail.sitek.net (megz@t2-30.sitek.net [212.34.33.93])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id XAA28837
for [REDACTED]; Sun, 23 Apr 2000 23:26:21 +0400 (MSD)
Date: Sun, 23 Apr 2000 23:24:16 -0700
From: [REDACTED]
X-Mailer: The Bat! (v1.029) S/N 83DA2C20
Reply-To: [REDACTED]
Organization: Internet Security
Priority: Normal
Message-ID: <8975.000423@doctor.com>
To: "fgeluso" [REDACTED]
Subject: Monday 23.04.2000
References: <002101bfa8af\$aeblbc10\$05f188cd@frankgvp>
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-RCPT-TO: [REDACTED]
X-UIDL: 254610730
Status: U

b6
b7C

Hello [REDACTED]

Hello, it's monday now of 23 april 2000

full week no answer from u.

waitinng for any reply

Best regards,

mailto:[REDACTED]

FROM [REDACTED] HEADERS
Received: from mail.sitek.net [212.34.32.37] by mail.fsiv...s.com with ESMTP
(SMTPD32-6.00) id AE083AF0218; Sat, 22 Apr 2000 04:08:48 -0400
Received: from mail.sitek.net (megz@t1-26.sitek.net [212.34.32.89])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id MAA22439
for [REDACTED]; Sat, 22 Apr 2000 12:08:37 +0400 (MSD)
Date: Sat, 22 Apr 2000 12:06:35 -0700
From: [REDACTED]
X-Mailer: The Bat! (v1.029) S/N 83DA2C20
Reply-To: [REDACTED]
Organization: Internet Security
Priority: Normal
Message-ID: <15504.000422@doctor.com>
To: [REDACTED]
Subject: WHY there is still no answer ?
References: <002101bfa8af\$aeblbc10\$05f188cd@ [REDACTED]>
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-RCPT-TO: [REDACTED]
X-UIDL: 254610724
Status: U

Hello [REDACTED]

Hello, i was sent u info about other 50% but still no answer from u.
waiting for reply

Best regards
[REDACTED]

mailto:[REDACTED]

b6
b7c

[redacted]
From: [redacted]
To: <techsupport@fsiwebs.com> [redacted]
Sent: Wednesday, April 19, 2000 5:50 AM
Subject: Your friend [redacted]

Hello [redacted]

b6
b7C

Ok, i see [redacted] have some family troblz, so i am givving u other 50% of your security problemz / and reccomendation on patching system.

First of all how is about [redacted]? i see u didn't make full patch on this computer.

Now, Do u know about DC ? (Domain controller) - i think u know.. SO, u also know that by default all nt computerz is as PDC (Primary Domain Controller). Now.. there is exist BDC (Backup Domain Controller) . - so i can make my computer as BDC if i know admin login/password. And the problem of your security is in chousing passwordz.

FsiWebs

I can just make bruteforce attack to your any computer and in ~15hourz can know password of admin (if your password include only A-Z,1-0). Now, all hackerz i know don't use bruteforce attack with simbols like %\$#^*&(~'

Here is rulez about chousing password.

- 1) Password must be between 9 to 15 characterz. (NOT MORE that 15!!!! - it's Important) if more that 15 i can decode it in 1 min ;) (it's mIcRoSoFt bug ;)
- 2) Password must include any 2 simbols of !@#\$%^&*()_+[]{}....and othgez...
- 3) don't use SAME passwordz on all computerz.
for example if one computer is xxx.xxx.xxx.56 other is xxx.xxx.xxx.27 - chose password of admin like:
for .56 - " crazy\$56Hack' " and for .27 - " crazy\$27Hack' "

But don't chouse like: " crazy\$Hack'56 " and " crazy\$Hack'27 "

have u understand this rule ? it's really important.

- 4) Don't give admin rights to more then 2 userz on one computer.

here is one knowhow (it know maximum 0.01% of ppl in the internet:
To protect all your computerz from any bruteforce attacks :

Create user with name '@' and password \$ANYPASSWORD\$, where

ANYPASSWORD - your random password from your head ;).

I think it's all, but after u will make this rule - i will scan your network again and will try to hack u with all known methodz. i think i will give u some more rulez. But anyway i need to talk with u in internet.

ps. hmmm think u can xfer me last 2k\$.

waiting for time/date when will we meet on the NET !!!

Cya body, and take care

Best regards,

mailto:

b6
b7C



E
S
S
E
N
T
I
A
L
I
N
F
O
R
M
A
T
I
O
N

[redacted]
From:

To:

Sent: Tuesday, April 18, 2000 6:27 PM

Subject: I have got money.

u
Hello [redacted]

z
We need to talk on the net.

u
how is about 15:00 your time ?

m
brb

u
z

Best regards,

[redacted]

mailto:[redacted]

b6
b7C



W
T
I
S
B
E
W

R
J
O
Y

E
R
E
H
W

From: [REDACTED]
To: [REDACTED]
Subject: FSI Wire Transfer
Date: Mon, 17 Apr 2000 15:04:50 -0400
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_NextPart_000_0005_01BFA87E.47593EC0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6700
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6700

This is a multi-part message in MIME format.

-----_NextPart_000_0005_01BFA87E.47593EC0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Hi [REDACTED]

still working on original patches.=20

Wire transferred Funds this afternoon at 3:00pm our time. However not =
without much difficulty.

Bank will only allow 1 wire transfer internationally per month. Had to =
fill out some additional paperwork
FSI Webs Take the bank some time to process.

Bank manager had trouble calling in wire transfer instructions, but you =
should receive your \$2K today :)

When you receive your \$, please e-mail all remaining patches/fixes to =
[REDACTED] AND mail to: [REDACTED]

Personal Note:

I have a family emergency and will be out of the office until next =
Monday.=20

If you must reach me, e-mail or leave a voice mail message.

When I get back on Monday: will talk about FUTURE.

[REDACTED]

-----_NextPart_000_0005_01BFA87E.47593EC0
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content=3D"text/html; charset=3Diso-8859-1" =
http-equiv=3DContent-Type>
<META content=3D"MSHTML 5.00.2920.0" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV>Hi [REDACTED] </DIV>
<DIV> </DIV>

Untitled

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTP (SMTPD32-6.00) id A4885FA0146; Thu, 13 Apr 2000 18:04:56 -0400

Received: from mail.sitek.net (t1-7.sitek.net [212.34.32.70]):

by mail.sitek.net (8.9.2/8.9.1) with SMTP id CAA05126

for [REDACTED] Fri, 14 Apr 2000 02:04:50 +0400 (MSD)

Date: Fri, 14 Apr 2000 02:02:53 -0700

From: [REDACTED]

X-Mailer: The Bat! (v1.029) S/N 83DA2C20

Reply-To: [REDACTED]

Organization: Internet Security

Priority: Normal

Message-ID: <585.000414@doctor.com>

To: "fgeluso" [REDACTED]

Subject: Re[2]: WHERE ARE U ?????

References: <005401bfa583\$3b1e17f0\$05f188cd [REDACTED]>

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: [REDACTED]

X-UIDL: 254610627

Status: U

Hello [REDACTED]

f> As you can see, we are making progress on your "patches", but they take time
f> to implement, as each machine is different and is taking more than 2 hrs.
f> Some Microsoft fixes causing us f...ckin headaches. Like we said, as soon as
f> these patches are complete, tomorrow or Monday, we'll xfer the \$2k.

Ok. i trust u man.

cya body

Best regards,

mailto:[REDACTED]

b6
b7c

b6
b7c

4_13_00_Headers

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTP
(SMTPD32-6.00) id A89B47630144; Thu, 13 Apr 2000 06:59:39 -0400
Received: from mail.sitek.net (t1-57.sitek.net [212.34.32.120])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id OAA05920
for <fgeluso@fsiwebs.com>; Thu, 13 Apr 2000 14:00:22 +0400 (MSD)
Date: Thu, 13 Apr 2000 13:58:22 -0700
From: [REDACTED]
X-Mailer: The Bat! (v1.029) S/N 83DA2C20
Reply-To: [REDACTED]
Organization: Internet Security
Priority: Normal
Message-ID: [REDACTED]
To: "FSIWEBS" [REDACTED]
Subject: WHERE ARE U ?????
References: <001501bfa3c9\$60938da0\$09f188cd@fsiwebs.net>
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-RCPT-TO: [REDACTED]
X-UIDL: 254610617
Status: U

Hello Fsiwebs,

Hi i see u have patched [REDACTED] ..and some others computers for
IIS attacks.
But we was talked about u will send 2k\$ on wensday - thursday. and
what i see ? now anything ...

But anyway i will wait for your reply for 24 hourz.

cya

Best regards,

mailto:[REDACTED]

b6
b7C



[REDACTED] EMAIL 4_11_2000

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTP

(SMTPD32-6.00) id AF191A031A; Tue, 11 Apr 2000 15:38:01 -0400

Received: from mail.sitek.net (t1-30.sitek.net [212.34.32.93])

by mail.sitek.net (8.9.2/8.9.1) with SMTP id XAA09271

for [REDACTED]; Tue, 11 Apr 2000 23:37:56 +0400 (MS

D)

Date: Tue, 11 Apr 2000 23:35:05 -0700

From: [REDACTED]

b6
b7c

X-Mailer: The Bat! (v1.029) S/N 83DA2C20

Reply-To: [REDACTED]

Organization: Internet Security

Priority: Normal

Message-ID: <15982.000411@doctor.com>

To: "FSIWEBS" [REDACTED]

Subject: Re[2]: FSI

References: <001501bfa3c9\$60938da0\$09f188cd@fsiwebs.net>

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: [REDACTED]

X-UIDL: 254610592

Status: U

Hello Fsiwebs,

F> How are you doing? Sorry not to get in touch with you sooner, but I

F> am still working on your suggestions. (They are a lot of work, and there

F> are lots of machines here.)

AN I know it ;) work work. ...

F> I cant use the other 50% untill I finish with what you already gave me.

F> Everyone is working on it, but it will still take

F> a few more days. We should be ready Friday or Monday. Then Ill send you

A F> the next \$2K, and you can send us the other 50%.

Ok no problem, i will look your network when will u finish 50% and will check is everithink is ok...

F> BTW, I thought our

F> agreement was that you would tell me what files you got, Im not trying to

F> change the rules, just go by what we said. My Boss wants it, I think he is

F> afraid that someone may sue us.



OK.

EMAIL 4_11_2000

i will show u some dirs of your files that i have. i have very much, but it's difficult to stand up all i have.

i think u understanding what is MUCH info...and how it's difficult to understand what and

but anyway:

1) first of all i have all gzipped dir of :

08/02/96 02:12p <DIR>

On your JUMBO (i will remember it [redacted] disk E:
IT'S VERY BIG...like 5 gb gzipped

b6
b7C

2) from SERVER1 [redacted] from disk D:

02/17/00 10:42a <DIR> CustSvc <-- 'this full dir.
gzipped.. ;)

3) from [redacted] I have all cybercash keys and mck...
and all files that have name Backup_Orders.txt with info like.. :

Bill To Name
Bill To E-mail
Bill To Address1
Bill To Address2
Bill To City
Bill To State
Bill To Zip Code
Bill To Phone
Bill To Fax
Ship To Name

[redacted]
:Same as Billing?

Comments : ?

Bill To CC Type :Visa?

Bill To CC Expire :11/00?

Bill To CC Number [redacted]

BUT i dont't need this info...and will not share it.

4) from [redacted] sql database

5) sql database from [redacted] (From disk C: and disk D:)
do u need i will continue ? it's hard for me and don't have enoth
time

b6
b7C

cya. waiting for 2k



EMAIL 4_11_2000

b6
b7C

Best regards,



mailto:



Received: from [redacted] by mail.fsiwebs.com
with ESMTP

(SMTPD32-6.00) id A1D012A01BE; Mon, 10 Apr 2000 15:56:00 -0400
Received: from [redacted] (stan.oib.com [redacted])
by [redacted] (8.9.3/8.9.3) with SMTP id PAA04671
for [redacted] Mon, 10 Apr 2000 15:55:54 -0400
(EDT)

Date: Mon, 10 Apr 2000 23:52:04 -0700
From: [redacted]
X-Mailer: The Bat! (v1.029) S/N 83DA2C20
Reply-To: [redacted]
Organization: Internet Security
Priority: Normal
Message-ID: <13994.000410@doctor.com>
To: [redacted]
Subject: this is [redacted]
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-RCPT-TO: [redacted]
X-UIDL: 254610574
Status: U

b6
b7c

Hello ,

hey hi, what's up ?
how is going with 50% of my reccomendations ?
I ready to give u other 50% and also we need to talk. and dc
rget to make xfer of 2k\$ to my bank account.

cya body

Best regards,

mailto:[redacted]

NEXT

Received: from [redacted] by mail.fsiweb
with ESMTP
(SMTPD32-6.00) id A1BCD8026C; Mon, 10 Apr 2000 15:55:40 -0400
Received: from [redacted] (stan.oib.com [redacted])
by [redacted] (8.9.3/8.9.3) with SMTP id PAA286
Mon, 10 Apr 2000 15:55:34 -0400 (EDT)
Date: Mon, 10 Apr 2000 23:53:38 -0700
From: [redacted]
X-Mailer: The Bat! (v1.029) S/N 83DA2C20
Reply-To: [redacted]

b6
b7c

Organization: Internet Security
Priority: Normal
Message-ID: <17995.000410@doctor.com>
To: [redacted] tech-support@fsiwebs.com, sales@fsiwebs.com,
webmaster@fsiwebs.com
Subject: re
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-RCPT-TO: <webmaster@fsiwebs.com>
X-UIDL: 254610573
Status: U

Hello ,

hey hi, what's up ?
how is going with 50% of my reccomendations ?
I ready to give u other 50% and also we need to talk. and
don't forget to make xfer of 2k\$ to my bank account.

b6
b7C

cya body

Best regards,

mailto:[redacted]

NEXT

Received: from [redacted] by mail.fsiwebs.com with ESMTP

(SMTPD32-6.00) id A172D2026C; Mon, 10 Apr 2000 15:54:26 -0400

Received: from [redacted] (stan.oib.com [redacted])
by [redacted] (8.9.3/8.9.3) with SMTP id PAA23018
for [redacted] Mon, 10 Apr 2000 15:54:21 -0400
(EDT)

Date: Mon, 10 Apr 2000 23:52:04 -0700

From: [redacted]

X-Mailer: The Bat! (v1.029) S/M 83DA2C20

Reply-To: [redacted]

Organization: Internet Security

Priority: Normal

Message-ID: <13994.000410@doctor.com>

To: [redacted]

Subject: this is [redacted]

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

b6
b7C

Mailbox:
Main

From: [redacted] Save Address

Message:
3 of 17

- Logoff
- Menu
- Compose
- Summary
- Search
- Help

Date: Sat, 8 Apr 2000 18:58:13 -0700
Reply-To: [redacted]
To: [redacted]
Subject: other 10% for security...

b6
b7C

Hello [redacted]

Ok..

Now check all computers for function:

It must be in TCP/IP setting for your TCP/IP protocol --- WINS --
U must set up DISABLE NETBIOS over TCP/IP.

coz if u will not set up it - anyone can scan your computers for
logins u have and for shares.
with this set key it will be impossible.

ok, Now it's full 50%.
I am going to prepair other 50% - it will be much difficult. but till
wensday i will prepair all documentation with how to close this
holes...

and also i think u can xfer to me other part of money (2000\$) for
future setting up security

cya

Best regards,

[redacted]

mailto:[redacted]

b6
b7C

[Next](#) [Previous](#) [Reply](#) [Reply All](#) [Forward](#) [Delete](#) [Move To](#)

[Sent](#) ▼

[Logoff](#) [Menu](#) [Compose](#) [Summary](#) [Top](#)

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTTP

(SMTPD32-6.00) id AA995302A4; Fri, 07 Apr 2000 18:00:57 -0400

Received: from mail.sitek.net (megz@t1-16.sitek.net [212.34.32.79])

by mail.sitek.net (8.9.2/8.9.1) with SMTP id CAA23954;

Sat, 8 Apr 2000 02:00:27 +0400 (MSD)

Date: Sat, 8 Apr 2000 01:58:33 -0700

From:

X-Mailer: The Bat! (v1.029) S/N 83DA2C20

Reply-To:

Organization: Internet Security

Priority: Normal

Message-ID: <382.000408@doctor.com>

To: tech-support@fsiwebs.com, sales@fsiwebs.com,

webmaster@fsiwebs.com

CC: tech-support@fsiwebs.com, sales@fsiwebs.com,

webmaster@fsiwebs.com

Subject: ??????????

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: <webmaster@fsiwebs.com>

X-UIDL: 254610543

Status: U

Hello

Hey, DO U NEED MY HELP IN PROTECTION ? OR I LOSTING MY TIME ????

U was said me that u are interested in my professional HELP ?!

Don't forget that u owe me 4k\$. and i will WORK .

I am not fucking ripper or something else, i am working for REAL and for FUTURE.

And i am interesting in working with u cause i have much projects.

I WAITING FOR YOUR REPLY

Best regards,

mailto:

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with SMTP

b6
b7C

(SMTPD32-6.00) id A8BD262023C; Fri, 07 Apr 2000 23:34:21 -0400
Received: from mail.sitek.net (megz@t1-56.sitek.net [212.34.32.119])

by mail.sitek.net (8.9.2/8.9.1) with SMTP id HAA04859
for [REDACTED] Sat, 8 Apr 2000 07:34:13 +0400

(MSD)

Date: Sat, 8 Apr 2000 07:32:18 -0700

From: [REDACTED]

X-Mailer: The Bat! (v1.029) S/N 83DA2C20

Reply-To: [REDACTED]

Organization: Internet Security

Priority: Normal

Message-ID: <0314_000408@doctor.com>

To: [REDACTED]

Subject: Re[2]: STEP #1 against Hacker attacks

References: <200004071702.AA65958@mail.fsiwebs.com>

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: [REDACTED]

X-UIDL: 254610546

Status: U

Hello [REDACTED]

[REDACTED]

[REDACTED] We received your email, sorry we missed you on ICQ this morning.

.....
[REDACTED] We will start work on the 40% you sent us, but I thought we agreed on 50%.
yes we agreed 40% but i can't tell u about other 10% u need to be at the computer when i will tell you about other holes. Coz i must to show u it.

[REDACTED] When can we expect the other 10% and a list of the files that you downloaded

b6
b7C

[REDACTED] from our machines.

Why u need file lists ? we was agreed about 5000\$ for the 200% security of your comuter network and now u asking me to show u

all what i have /?!

i CAN DO IT IT'S NO PROBLEM, BUT I CANT UNDERSTAND WHY U ASKING TH IIS

MATERIALS FROM ME?

[] What we have will take a few days to implement. Will be online again

b6
b7c

FG> Wednesday morning around 9:30 am our time on ICQ.

Wensday ???? why not on Monday. i hate to wait.
I am ready to set up of security for your network !

cya, waiting for reply

Best regards,

[]

mailto:[]

4/7/00 ICQ



hi, now time in russia is 1:00 am (night)
I have i had ake, and will send u some information via email.
We will talk tomorrow. but cat we do it on the morning your time ?

hi, have u recieved my email yesturday ? why there is no answer ?
still waiting for u



b6
b7C

We received your email, sorry we missed you on ICQ this morning.

We will start work on the 40% you sent us, but I thought we agreed
on 50%. When can we expect the other 10% and a list of the files
that you downloaded from our machines.

What we have will take a few days to implement. Will be online aga
in Wednesday morning around 9:30 am our time on ICQ.

cya,



From: [REDACTED]

b6
b7C

Date: Fri, 7 Apr 2000 01:20:38 -0700

Reply-To: [REDACTED]

To: [REDACTED]

Subject: STEP #1 against Hacker attacks

Hello [REDACTED]

Hi, this is document , read it and we will talk more.

1. Install SP6a

www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.as

p

U think it all ? haha

2.

First of all download

www.microsoft.com/security/products/iis/CheckList.exe

(It's zipped .html documet, that will teach you how to make protection from all known IIS holes.

Make it on your ns.fsiwebs.com (really i can still have access to it.)

and on other NT mashines, that have adapter with non intranet addresses.

I think it will take from u about 1 -2 hour...

3.

Install NT Option Pack

www.microsoft.com/ntserver/nts/downloads/recommended/NT4OptPk/default.asp

4.

Install MDAC 2.1 SP2

www.microsoft.com/data/download_21242023.htm

5.

Now.....

Apply the following additional Registry Keys:

```
HKEY_LOCAL_MACHINE\SYSTEM\  
CurrentControlSet\Control\FileSystem  
NtfsDisable8dot3NameCreation  
REG_DWORD=1
```

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\W3SVC\Parameters
SSIEnableCmdDirective
REG_DWORD=0

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\AFD\Parameters
DynamicBacklogGrowthDelta
REG_DWORD=10

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\AFD\Parameters
EnableDynamicBacklog
REG_DWORD=1

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\AFD\Parameters
MinimumDynamicBacklog
REG_DWORD=20

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\AFD\Parameters
MaximumDynamicBacklog
REG_DWORD=(not to exceed 5000 for each 32MB RAM)

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\Tcpip\Parameters
EnableDeadGWDetect
REG_DWORD=0

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\Tcpip\Parameters
EnableICMPRedirect
REG_DWORD=0

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\Tcpip\Parameters
EnablePMTUDiscovery
REG_DWORD=0

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\Tcpip\Parameters
KeepAliveTime
REG_DWORD=300000

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\Tcpip\Parameters

IGMPLEVEL
REG_DWORD=0

6.
now about your NetBios....

Unbind NetBIOS from TCP/IP on the Internet connected NIC.

Got to Control Panel ==> Network --> Bindings.
Choose to View Bindings for "All Adapters".
Expand each adapter.
Highlight "WINS Client(TCP/IP)" for the Internet
connected interface and select 'Disable'.

huh i have very fucking head ake

Here is i think 40% of your security problems... but not all ;)

cya tomorrow morning prefer your time

Best regards,

[Redacted Signature]

mailto:

[Redacted Email Address]

b6
b7C

Here..
To The Director of FSIWEBS

Dear Sear,

Hi this is again your favorite HACKER [REDACTED]

b6
b7c

I can't understand YOU interested in my HELP or you just spend my time ??? or Fucking my brains.

I was talked with [REDACTED] and I was accepted the deal about 5000\$ for HELPING with your SECURITY [REDACTED] nice guy... He was not answered me today, and no money on my bank account. (I was agreed that first part is 1000\$).

I WILL WAIT TILL TOMORROW, and if I will not see any motion from your side, I will put credit card information (example from www.ePhonecard.com to Popualr web site (like www.porshe.com ;) or if u don't like CAR servers ..to some large web hosting.) , and will email to EPHONE, that your company don't want to pay me for SECURITY) And if it will not help u in deciding for FAST work without losing my TIME – I will... i think u can imigene it yourself without MY HELP. Or I must email / fax /call to your BANK customers and say them about your SHIT security ????

Look, I interested to work with U, coz I see the future. BUT I don't SEE that u are interested

CYA, AND TAKE CARE, I AM WAITING FOR RESPONSE to my EMAIL or ICQ : [REDACTED]

Best regards,

[REDACTED]
FAX : 1-201-221-8175

Contact Email: [REDACTED]

b6
b7c

ICQ 4/04

i am going to SLEEP now, i think u have received my FAX and will r
eplly me ASAP. and i also think that i will see 1000\$ on my bank ac
count.
cya

ICQ 4/05

[] Hi [] we have wired your money today. How long do you think
it will take for you to receive ?

[] when was u xfered money ?
and have u made FAST xfer or regular ?

[] Document shows bank sequence # 4628

[] ok. i will wait for money income.

b6
b7c

[] Money was wired at 1:50pm our time

[] can we talk about futere work ?

[] we want to talk about what you will do for us when you receive
money. let me know when you receive money.

[] ok i think money will be tomorrow or the day after tomorrow

- 1) i will not publish any of your info to anywhere in the internet
. Nobody will know that u was been hacked.
- 2) I will say u 50% of your holes. and will teach u how to make pr
otection.
- 3) Will give u consult of chousing passwords ;) couse password in
your db like athens1896 very BAD choise

[] OK [] please ICQ me when you get the money. Usual time.
cya

b6
b7c

[] ok. No problem.

when was u xfered money ?
and have u made FAST xfer or regular ?

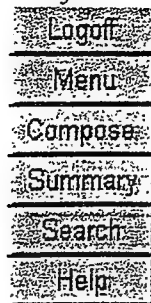
have u entered all correctly ? can i see payment document that gav
e u bank when u was made xfer ?

Mailbox:

Main

Message:

10 of 12



From:

[Redacted]

Save Address

Date: Sun, 2 Apr 2000 04:28:34 -0700

Reply-To:

[Redacted]

To: [Redacted] tech-support@fsiwebs.com, sales@fsiwebs.com,
webmaster@fsiwebs.com

Subject: hi pplz. it's [Redacted]

Hello [Redacted]

I was browse on the links that u are providing on your website...
i mean <http://www.bank2000.com/HOTLINKS/>

I belive in future of work with u. Couse i really want to orginize
company like "Internet Security Company".. and may be u will help
me to do it.

I can share with your info, but will not do it. I am not villian ;)

Need to talk to u asap.

will be on the Net on monday...usially time /..
cya

Best regards,

[Redacted]

mailto:

[Redacted]



failed



Enter secure mode.

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTTP

(SMTPD32-6.00) id A982500168; Thu, 30 Mar 2000 13:14:26 -0500

Received: from mail.sitek.net (megz@t1-41.sitek.net [212.34.32.104])

by mail.sitek.net (8.9.2/8.9.1) with SMTP id WAA31278;

Thu, 30 Mar 2000 22:14:16 +0400 (MSD)

Date: Thu, 30 Mar 2000 22:12:31 -0800

From: [REDACTED]

X-Mailer: The Bat! (v1.029) S/N 83DA2C20

Reply-To: [REDACTED]

Organization: Internet Security

Priority: Normal

Message-ID: <16925.000330@doctor.com>

To: [REDACTED] tech-support@fsiwebs.com, sales@fsiwebs.com,

webmaster@fsiwebs.com

Subject: Hello my friendz

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: <webmaster@fsiwebs.com>

X-UIDL: 252953773

Status: U

Hello [REDACTED]

So, there is in your country now 10 am

I am waiting for your response for 2 hours, if there will be no

response with answer YES , we accept your conditions.

After 2 hours from this moment my price for my HELP will increase * 2.

So, if i will not receive answer in 4 hours i will begin my skill

...

Look, i want to help u, coz if not me - someone else will enter into

your system, and then u will remember me ... when all your computers

will go down.

remember only HACKERz know how to protect network...

ps. and don't try call interpol and fbi, they will not help u.

if i will know about it that u have done it - i will post your confidential info to much servers and some NEWS servers in Intern

et.

Cya

Best regards,



mailto:



b6
b7C

Message

From:

Date:

[redacted]
3/30/00 5:17 PM

fuck u need 30 sec to download it and install
don't lose time

and i will repeat don;t fuck my brains with sometimes stupid thingz

Message

From:

Date:

[redacted]
3/30/00 5:08 PM

haha ;)

i can install backdoor not from your computer. your system is fully holled . and Wee need to solve money problem.

And we must do it now. coz if not - ... u know..

Message

From:

Date:

[REDACTED]
3/30/00 5:04 PM

u want me to talk over the phone ?
why u need it

- 1) u will never will able to trace me
 - 2) i have bad english
-

[REDACTED] ICQ History Events

Message

From:

Date:

[REDACTED]
3/30/00 4:11 PM

Yes u can.

And + after will we make deal i can work with u - so free consulting and all that u want .

Message

From:

Date:

[REDACTED]
3/30/00 4:06 PM

What is your answer of my deal ?

I will fix all your HOLES in your network and will not share your secured information.

The price on this moment is $3 * 2 = 6\ 000\ \$$

[redacted]
From: [redacted]
Sent: Thursday, March 30, 2000 3:46 AM
To: [redacted]
Cc: tech-support@fsiwebs.com; sales@fsiwebs.com; webmaster@fsiwebs.com
Subject: It's me Again... your lover hacker

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTP
(SMTPD32-6.00) id AC042CD01B0; Wed, 29 Mar 2000 15:48:04 -0500

Received: from mail.sitek.net (megz@t1-3.sitek.net [212.34.32.66])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id AAA23704;
Thu, 30 Mar 2000 00:47:59 +0400 (MSD)

Date: Thu, 30 Mar 2000 00:46:16 -0800

From: [redacted]
X-Mailer: The Bat! (v1.029) S/N 83DA2C20

Reply-To: [redacted]
Priority: Normal

Message-ID: <1832.000330@doctor.com>

To: [redacted]
Cc: tech-support@fsiwebs.com, sales@fsiwebs.com, webmaster@fsiwebs.com

Subject: It's me Again... your lover hacker

Mime-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-RCPT-TO: <webmaster@fsiwebs.com>

X-UIDL: 247083732

Status: U

Hello [redacted]

I have forgot, that i have all your SQL and ORACLE databases...
and if today there is will no answer to the fax or to this email i will
send to all your customers info that u was been hacked and u don't
want to pay us 3000\$ for making your network security. Alsow i will
find some newspapers in NJ that will be interested to write about u
;)

cya

And don't forget if u will decide to do it tomorrow - it will be
6000\$
and my icq number (if u want to talk to me) is 5439224 ... i am online

cya

Best regards,

mailto:[redacted]

b6
b7C

b6
b7C

10 The Director of FSIWEBS

Dear Sear,

I present the company on provision of safety work in Internet.

I can Say you that you have been hacked by group of Hackers, and this group of Hackers still have access to your system. And they already have very much information for your all computer network.

Your computer Network consist from Local intranet [REDACTED]
[REDACTED]. This hacker group know a lot of your business and they was been (and still ...) in your computer network about 2 months...

b6
b7C

Also we have credit card information of all your clients, and cybercash keys for access to your Merchant. For example all orders of clients on [REDACTED] store in Backup_orders.txt

We can Help you in decision on a matter of know is your Network easy to hack and are your computers and main server 100% saved from hacker attacks. If it not saved we can fix all holes in your Network.

We Will protect your Network with 200% guarantee. So nobody will never enter to your network without your permission.

Our work will cost for your network \$3 000 . Think - so little money for 200% security.

Who we are - Our command is professional hackers and certificated programmers by Microsoft, Cisco, Novell.

Only hackers can protect your network with 100% security level.

In case of decline our suggestion the cost of Unpublishing YOUR CONFIDENTIAL INFORMATION will increase *2 .

Waiting for your reply TODAY. //

Best regards,

[REDACTED]
FAX : 1-201-221-8175

Contact Email: [REDACTED]

b6
b7C

[REDACTED]
From: [REDACTED]
Sent: Thursday, March 30, 2000 2:25 AM
To: [REDACTED] tech-support@fsiwebs.com; sales@fsiwebs.com;
webmaster@fsiwebs.com
Subject: HACKERZ

Received: from mail.sitek.net [212.34.32.37] by mail.fsiwebs.com with ESMTP
(SMTPD32-6.00) id A99F15F1002C; Wed, 29 Mar 2000 14:29:35 -0500
Received: from mail.sitek.net (megz@t1-56.sitek.net [212.34.32.119])
by mail.sitek.net (8.9.2/8.9.1) with SMTP id XAA19567;
Wed, 29 Mar 2000 23:29:24 +0400 (MSD)
Date: Wed, 29 Mar 2000 23:24:44 -0800
From: [REDACTED]
X-Mailer: The Bat! (v1.029) S/N 83DA2C20
Reply-To: [REDACTED]
Priority: Normal
Message-ID: <2975.000329@doctor.com>
To: [REDACTED] tech-support@fsiwebs.com, sales@fsiwebs.com,
webmaster@fsiwebs.com
Subject: HACKERZ
Mime-Version: 1.0
Content-Type: text/plain; charset=koi8-r
Content-Transfer-Encoding: 8bit
X-RCPT-TO: <webmaster@fsiwebs.com>
X-UIDL: 247083731
Status: U

b6
b7C

Hello ,

To The Director of FSIWEBS

Dear Sear,

I present the company on provision of safety work in Internet.

I can Say you that you have been hacked by group of Hackers,
and this group of Hackers still have access to your system.
And they already have very much information for your all
computer network.

Your computer Network consist from Local intrane [REDACTED]

[REDACTED] to
INTERNET SERVERS (u know which are...) ...

This hacker group know a lot of your business and they was
been (and still ...) in your computer network about 2
months...

Also we have credit card information of all your clients, and
cybercash keys for access to your Merchant. For example all
orders of clients on [REDACTED] store in Backup
orders.txt

We can Help you in decision on a matter of know is your
Network easy to hack and are your computers and main server
100% saved from hacker attacks. If it not saved we can fix all
holes in your Network.

We Will protect your Network with 200% guarantee. So nobody

will never enter to your network without your permission.

Our work will cost for your network \$1200 . Think - so little money for 200% security.

Who we are - Our command is professional hackers and Certified programmers by Microsoft, Cisco, Novell.

Only hackers can protect your network with 100% security level.

In case of decline our suggestion the cost of Unpublishing YOUR CONFIDENTIAL INFORMATION will increase *2 .

Waiting for your reply TODAY to our fax or Email. //

Best regards,

FAX : 1-201-221-8175

Contact Email

b6
b7C

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/25/2000

To: Counterterrorism
Criminal Investigative

Attn: [redacted] SSA [redacted]
SSA [redacted]
Undercover and Sensitive
Operations Unit, SSA
[redacted]

New Haven
Newark
Seattle

SA [redacted]
SA [redacted]
SSA [redacted]
FM [redacted]

b3
b6
b7C
b7E

From: Seattle
Squad 11

Contact: SA [redacted] 206/262-2432

Approved [redacted]

Drafted B [redacted]

Case ID # [redacted]

(X)

Title: FLYHOOK

Synopsis: Provide FBIHQ with information needed for budget enhancement.

Reference: [redacted]

b3
b6
b7C
b7E

Details: Seattle is currently conducting a Group II undercover operation (UCO) entitled FLYHOOK in coordination with six other field offices. A total of [redacted] is needed for the UCO. When originally approved, the UCO was attempting to lure one Subject from Russia. In a consensually recorded telephone call with the Subject on [redacted] the Subject stated [redacted]

[redacted]

SEARCHED _____	INDEXED _____
SERIALIZED _____	FILED _____
AUG 30 2000	
FBI-SEATTLE	

[redacted]

To: Counterterrorism From: Seattle
Re: [REDACTED] 08/25/2000

b3
b7E

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

Set Lead 2:

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

Read and clear.

Set Lead 3:

NEW HAVEN

AT NEW HAVEN

Read and clear.

Set Lead 4:

NEWARK

AT FRANKLIN TOWNSHIP

Read and clear.

23 [REDACTED] 01.ec
♦♦

b6
b7C

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/21/2000

On an E-mail was sent from E-mail address

b6
b7C
b7E

Investigation on 06/21/2000 at Seattle, WA

File Date dictated 06/21/2000

by SA

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/01/2000

On [redacted] an E-mail was received at E-mail address [redacted] from [redacted] using the E-mail address [redacted] of [redacted]. The E-mail stated [redacted] would send his [redacted]

b6
b7C
b7E

On [redacted] E-mailed his resume from the E-mail address of [redacted]. It showed [redacted] address as [redacted] and his home telephone number as [redacted]. A copy of each E-mail is attached and considered part of this FD-302.

Investigation on 07/01/2000 at Seattle, WAFile # [redacted] Date dictated 07/01/2000by SA [redacted]b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/07/2000

On an E-mail was sent from the E-mail

b6
b7C
b7E

Investigation on 07/07/2000 at Seattle, WA

File # Date dictated 07/07/2000

by SA

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/09/2000

On two E-mails were received at E-mail

b6
b7C
b7E

Investigation on 07/09/2000 at Seattle, WA

File Date dictated 07/09/2000

by SA

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/11/2000

On an E-mail was received at E-mail

b6
b7C
b7E

Investigation on 07/11/2000 at Seattle, WA

File # Date dictated 07/11/2000

by SA

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/27/2000

On an E-mail was sent from E-mail address

b6
b7C
b7E

Investigation on 07/27/2000 at Seattle, WA

File # Date dictated 07/27/2000

by SA

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/28/2000

On an E-mail was received at E-mail

b6
b7C
b7E

Investigation on 07/28/2000 at Seattle, WA

File # Date dictated 07/28/2000

by SA

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/08/2000

On an E-mail was sent from E-mail address

b6
b7C
b7E

Investigation on 08/08/2000 at Seattle, WA

File # Date dictated 08/08/2000

by S.

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/15/2000

On [redacted] an E-mail was received at E-mail [redacted]
[redacted] It provided the following information
needed to obtain a visa:

b6
b7C
b7E

Surname
Given names
Nationality
Date of birth
City
Country
Sex
Passport Number

Male

[redacted] provided his home address as follows:

Country
City
Zip
Street
House
Flat

[redacted] also provided the following information for his
business partner:

Surname
Given names
Nationality
Date of birth
City
Country
Sex
Passport Number

Male

b3
b6
b7C
b7E

Investigation on 08/15/2000 at Seattle, WA

File # [redacted] Date dictated 08/15/2000

by SA [redacted]

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/17/2000

On an E-mail was sent from E-mail

b6
b7C
b7E

Investigation on 08/17/2000 at Seattle, WA

File # Date dictated 08/17/2000

by SA

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/17/2000

On an E-mail was received at E-mail

b6
b7C
b7E

Investigation on 08/17/2000 at Seattle, WA

File # Date dictated 08/17/2000

by SA

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/18/2000

On an E-mail was received at E-mail

b6
b7C
b7E

Investigation on 08/18/2000 at Seattle, WA

File # Date dictated 08/18/2000

by S.

b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/30/2000

To: Counterterrorism

Attn:

Los Angeles
Seattle

SSA
SA
SSA

SSA

From: Seattle

Squad 11

Contact: SA

206/262-2432

b3
b6
b7C
b7E

Approved By:

Drafted By:

Case ID:

(Pending)

Title:

Synopsis:

Details: Case Agent: SA
File #:

Case Title: FLYHOOK
Squad: 11

For information of on 8/30/99, FLYHOOK

b3
b6
b7C
b7E

To: Counterterrorism From: Seattle
Re: [REDACTED] 08/30/2000

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

b6
b7C
b7E

Set Lead 2:

LOS ANGELES

AT LOS ANGELES, CA

[REDACTED]

235 [REDACTED] 11.ec

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/25/2000

To: Seattle

Attn: SAC

UCC SSA

Salt Lake City

Attn: SAC

UCC

SA

From: Criminal Investigative

Operational Support Section (OSS), Undercover and
Sensitive Operations Unit (USOU), Room 4343

Contact: SSA (202) 324-3734

b3
b6
b7C
b7E

Approved By:

Drafted By:

Case ID # (Pending)

Title: FLYHOOK;
COMPUTER INTRUSION

Synopsis: FBIHQ authority for Special Agent (SA) Salt Lake City Division, to travel to Seattle, Washington, for temporary duty as an undercover agent (UCA) with respect to captioned matter.

Reference: Seattle electronic communication (EC) to FBIHQ/USOU, dated 08/01/2000.

Details: FBIHQ authority is granted for SA Salt Lake City Division, to travel to Seattle, Washington, for temporary duty as an UCA on captioned Group II investigation. SA is advised that this is a short term temporary duty assignment, requiring his participation for approximately one week during late August to early September 2000. SA is a certified UCA; however he must receive a safeguard assessment from the Undercover Safeguard Unit (USU) before taking part in any prolonged covert activity.

b3
b6
b7C
b7E

With regards to SA travel to Seattle, it is noted that the Seattle Division will assume all cost of travel and expenses incurred.

SACs Seattle and Salt Lake City concur with travel.

CC: 2 - Seattle
3 - Salt Lake City
9 - FBIHQ

♦♦

SAC
SSA

SEARCHED	INDEXED
SERIALIZED	FILED
AUG 31 2000	
FBI SEATTLE	

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/28/2000

To: Counterterrorism

Attn:

Little Rock
Los Angeles
New Haven

Newark
Sacramento
Seattle

Washington Field

	SSA	
	SSA	
	IOS	
SA		
SSA		
SA		
SA		
SA		
SA		
SA		
SA		
IOS		
SA		

b6
b7C
b7E

From: Los Angeles

SARA 3

Contact: SA

(714) 245-5297

Approved By:

Drafted By:

Case ID #:

b3
b6
b7C
b7E

Title: INSUR(S) aka

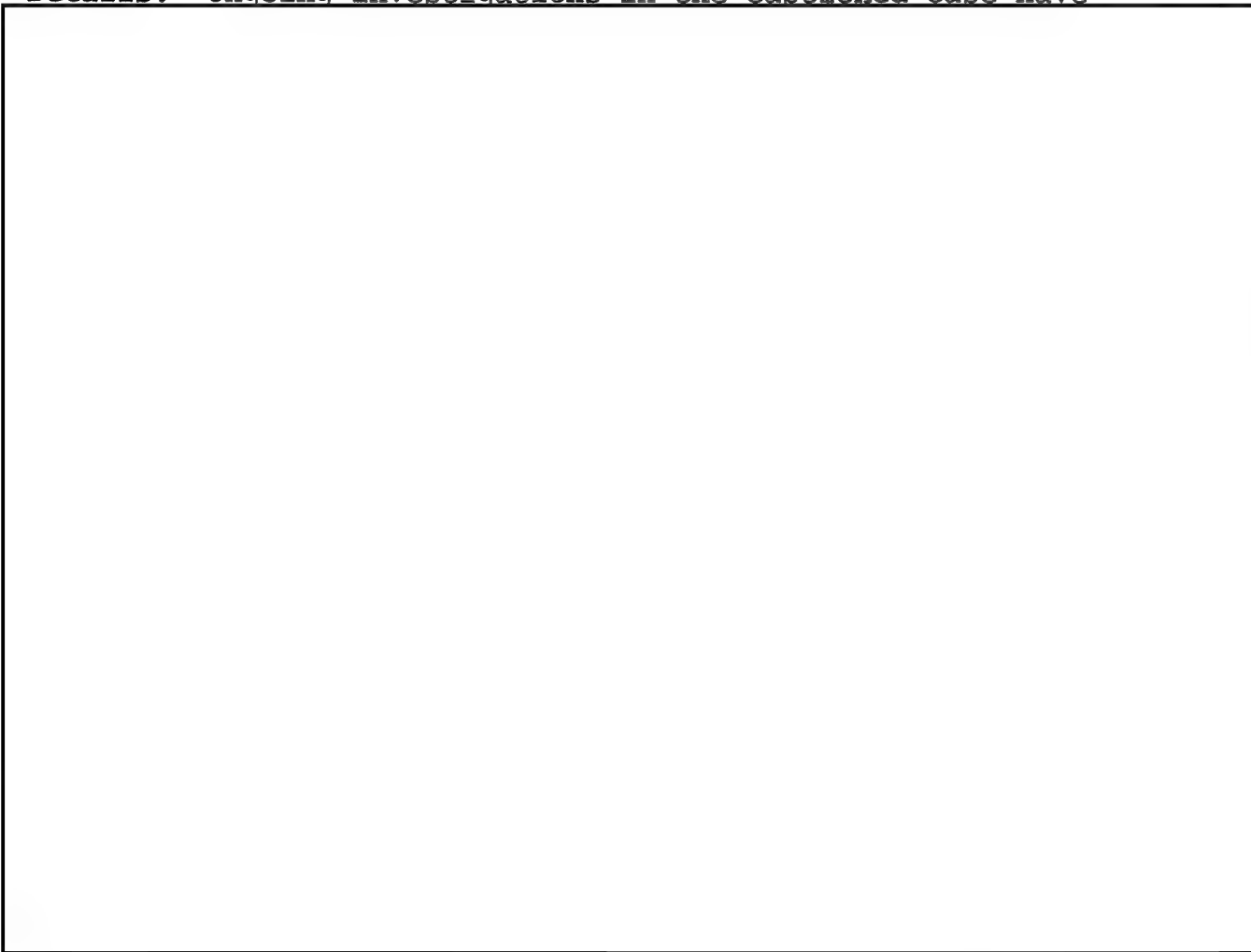
STERLING MICROSYSTEMS - VICTIM;
INTRUSION - INFO SYSTEMS;
OO:LOS ANGELES

Synopsis: To report on programs and exploits used by to intrude into the computer networks of Sterling Microsystems and CTS Network Services.

To: Counterterrorism From: Los Angeles
Re: [REDACTED] 08/28/2000

Enclosure(s): Enclosed for each receiving office is one computer disk containing a copy of [REDACTED] programs, an email explaining the intrusion at CTS and copies of the source code used for the intrusions at CTS.

Details: Ongoing investigations in the captioned case have



b3
b6
b7C
b7E

The source code for each of these backdoors is contained on the enclosed disk.

The initial intrusion into CTS's Unix system was through an exploit in the ftp daemon program that would allow a user to cause a ftpd core dump in which the passwords of the legitimate user were shadowed or hidden. These shadowed passwords are then un-hidden using a separate password breaking program. The broken passwords are then used to logon to the network and gain additional access.

To: Counterterrorism From: Los Angeles
Re: [REDACTED] 08/28/2000

b3
b6
b7C
b7E

Attached is an email between [REDACTED] of CTS and [REDACTED] that further explains the process.

To assist in the further identification of [REDACTED] and the linking of the referenced substantive case files, these programs and exploits are being made available to the captioned Case Agents for use as deemed appropriate in their respective investigations.

♦♦

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/30/2000

On an E-mail was sent from E-mail

b6
b7C
b7E

Investigation on 08/30/2000 at Seattle, WA

File Date dictated 08/30/2000

by SI

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/06/2000

On an E-mail with attachment was sent

b6
b7C
b7E

Investigation on 09/06/2000 at Seattle, WA

File # Date dictated 09/06/2000

by SA

b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 09/12/2000

To: Counterterrorism

Attn:

	SSA	
	SSA	
	IOS	
	AWS/AISU IOS	

Little Rock
Los Angeles

New Haven

Sacramento
Washington Field
Newark
Seattle

SA
SA
SA
SA
SA
SA
SA
SA

From: Seattle

Squad 11

Contact: SA

206-262-2436

Approved By

Drafted By:

Case ID #:

b6
b7C
b7E

Title: INSUB (S) aka

b3
b6
b7C
b7E

REGISTER NOW, ISSAQUAH, WA - VICTIM
CIDT/COMPUTER INTRUSION
THEFT OF INFORMATION

To: Counterterrorism From: Seattle
Re: [redacted] 09/12/2000

b3
b6
b7C
b7D
b7E

Synopsis: To provide for comparison purposes, electronic mail exchanged between [redacted] and Regnow, FBI Seattle victim company.

Enclosure(s): For each substantive case file, Copies of FD-302s with attachments, including: electronic mail from [redacted]

[redacted] to [redacted]
[redacted]

Details: The above captioned cases are believed to relate to an individual known as [redacted] and involve computer intrusion and extortion.

Register Now (Regnow) is a victim company located in Issaquah, Washington. Regnow is in the business of taking customer credit card information to register computer shareware. Regnow pays its clients through wire transfers. Regnow has credit card information for over 500,000 customers and bank/wire transfer information for over 3,000 clients.

In July, 2000, an individual claiming to be [redacted] of The Expert Group of Protection Against Hackers Attacks, contacted Regnow via e-mail. [redacted] had intruded into the Regnow server and taken the credit card and bank transfer information. [redacted] demanded \$25,000.00 in exchange for a promise not to release the information to the press. After a few telephone conversations and several e-mails, Regnow paid [redacted] \$10,000.00 through a Western Union wire transfer to another person, [redacted] claimed to have a partner, [redacted] [redacted] indicated that [redacted] is a Russian businessman able to take possession of the money in Moscow.

b6
b7C
b7D

To assist in finding similarities between the captioned cases, copies of [redacted] [redacted] are being made available to case agents.

To: Counterterrorism m From: Seattle
Re: [REDACTED] 09/12/2000

b3
b6
b7C
b7E

LEAD(s) :

Set Lead 1:

ALL RECEIVING OFFICES

Read and clear.

25 [REDACTED] 01.ec
♦♦

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/02/2000

[redacted]
[redacted]
telephone number [redacted] cellular telephone number [redacted]
[redacted] e-mail address [redacted] was interviewed at his
place of employment. Also present was [redacted]

[redacted] e-mail address

[redacted] After being advised of the identity of the
interviewing agents and the nature of the interview, he provided
the following information:

b6
b7C
b7D

b6
b7C
b7D

Investigation on 08/01/2000 at [redacted]

File [redacted]

Date dictated 08/02/2000by ☒ SA [redacted]**URGENT COPY**

b3
b6
b7C
b7D
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/03/2000

[redacted]
[redacted]
telephone number [redacted] cellular telephone number [redacted]
[redacted] e-mail address [redacted] was interviewed at his
place of employment. Also present was [redacted]

[redacted] e-mail address
[redacted] After being advised of the identity of the
interviewing agents and the nature of the interview, he provided
the following information:

[redacted]

b6
b7C
b7D

Investigation on 08/03/2000 at [redacted]

File # [redacted] Date dictated 08/03/2000

by SA [redacted]
SA [redacted]

b3
b6
b7C
b7D
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/08/2000

[redacted]
[redacted]
[redacted] telephone number [redacted] cellular telephone
number [redacted] e-mail address [redacted] was
interviewed at his place of employment. Also present was [redacted]
[redacted] e-mail
address [redacted] After being advised of the identity of
the interviewing agents and the nature of the interview, he
provided the following information:

b6
b7C
b7D**AGENT COPY**Investigation on 08/04/2000 at [redacted]

File # [redacted]

Date dictated 08/08/2000

by

S4
S4b3
b6
b7C
b7D
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/14/2000

[redacted]
[redacted]
[redacted] telephone number [redacted] cellular telephone
number [redacted] e-mail address [redacted] was
interviewed at his place of employment. Also present was [redacted]
[redacted] e-mail
address [redacted] and [redacted] [redacted] of
Register Now. After being advised of the identity of the
interviewing agents and the nature of the interview, she provided
the following information:

[redacted]

b6
b7C
b7DInvestigation on 08/09/2000 at [redacted]

File # [redacted]

Date dictated 08/10/2000by SA [redacted]
SA [redacted]**AGENT COPY**b3
b6
b7C
b7D
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/18/2000

[redacted]
[redacted]
[redacted] telephone number [redacted] provided Special Agent
(SA) [redacted] and SA [redacted] of the Seattle
Division of the Federal Bureau of Investigation (FBI) with the
following documents:

[redacted]

b6
b7C
b7DInvestigation on 08/18/2000 at [redacted]

File # [redacted]

Date dictated 08/18/2000

by

SA [redacted]
SA [redacted]**URGENT COPY**b3
b6
b7C
b7D
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 09/19/2000

To: Counterterrorism

Attn:

Los Angeles

Moscow

Newark

Seattle

St Louis

Washington Field

SSA

SARA-3 SA

ALAT

Franklin Township RA

SA

SA

SA

SA

From: New Haven

6

Contact: (203) 503-5041

Approved By

Drafted By

Case ID #:

b3
b6
b7C
b7E

Title: INSUR aka

Fug (B);

OIB, Inc. - Victim;

Impairment, Intrusion, Extortion

Synopsis: Indictment of subject.

Details: On 9/6/2000 a Federal Grand Jury for the United States District Court, District of Connecticut returned a 3 count indictment on captioned subject [redacted] was indicted for violations 18 U.S.C. Section 1951 [Interference in Commerce by Extortion], 18 U.S.C. Section 1030 (2) [Accessing a computer in excess of and without authorization] and 18 U.S.C. Section 1030 (7) [Extortion concerning a protected computer].

b3
b6
b7C
b7E

To: Counterterrorism From: New Haven
Re: 09/19/2000

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Read and clear.

◆◆

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 09/18/2000

To: Seattle

From: Seattle

Squad 11

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: FLYHOOK

Synopsis: Open subfile for financial matters.

Details: To better account for financial matters arising from this Group II UCO, it is recommended a subfile be opened. It is requested that [redacted] be opened.

26 [redacted] 01.ec
♦♦



File into as well

b3
b6
b7C
b7E

b3
b6
b7C
b7E

Open subfile

SEARCHED	INDEXED
SERIALIZED	FILED
SEP 22 2000	
FBI-SEATTLE	

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 10/03/2000

To: Counterterrorism

Attn:

SSA

From: Seattle

Squad 11

Contact: SA

206-262-2436

Approved

Drafted By

Case ID #

Title:

CIDTA/COMPUTER INTRUSION
CIDTA/THEFT OF INFORMATION

UNSUB. aka

aka

UNSUB. aka

THE EXPERT GROUP OF PROTECTION
AGAINST HACKERS ATTACKS;
REGISTER NOW (REGNOW.COM) - VICTIM
CIDTA/UNAUTHORIZED ACCESS;
CIDTA/THEFT OF INFORMATION

Synopsis: To forward consensually monitored tape recordings to
[redacted] for analysis.

Package Copy: Being forwarded under separate cover are four (4)
tape recordings from [redacted] and two (2) tape recordings
from [redacted]

Details: Enclosed for analysis are four (4) tape recordings from
the Register Now case, [redacted] and two (2) tape recordings
from the Flyhook case, [redacted] The tapes from Register
Now are consensually monitored telephone calls between [redacted]
[redacted] and a Russian male identifying himself
as [redacted] beleived to be [redacted] The tapes are dated
[redacted]

The tape from Flyhook dated [redacted] a CW
and a Russian male identifying himself as [redacted]

b3
b6
b7C
b7E

b3
b6
b7C
b7D
b7E

SERIALIZED	FILED
OCT 06 2000	
FBI SEATTLE	

To: Counterterrorism From: Seattle
Re: [REDACTED] 10/03/2000

However, a subsequent e-mail from [REDACTED] indicated that the Russian male was, in fact, [REDACTED]
The tape from Flyhook dated [REDACTED] is call between a UCA and a Russian male identifying himself as [REDACTED]

b3
b6
b7C
b7E

To: Counterterrorism From: Seattle
Re: [REDACTED] 10/03/2000

LEAD(s) :

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

These tapes are provided at the Request of SSA [REDACTED]
in order to make comparison to other consensually monitored
telephone calls from the related Russian computer extortion
cases.

♦♦ 277 [REDACTED] 02.ec

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/29/2000

On an E-mail was received at E-mail

b6
b7C
b7E

Investigation on 09/29/2000 at Seattle, WA

File # Date dictated 09/29/2000

by S

b3
b6
b7C
b7E